IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE APPLICATION FOR SEARCH AND SEIZURE WARRANTS OF:	
A CELLULAR TELEPHONE FURTHER DESCRIBED IN ATTACHMENT A-1	**Case No.** 22-mj-2893-AAQ
A WHITE 2005 CHEVROLET COLORADO FURTHER DESCRIBED IN ATTACHMENT A-2	**Case No.** 22-mj-2894-AAQ
HISTORICAL CELL SITE INFORMATION ASSOCIATED WITH PARTICULAR CELLULAR TOWERS	**Case No.** 22-mj-2895-AAQ **Case No.** 22-mj-2896-AAQ **Case No.** 22-mj-2897-AAQ **Case No.** 22-mj-2898-AAQ

UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Benjamin D. Parker, being first duly sworn, depose and state as follows:

PURPOSE OF THIS AFFIDAVIT

This affidavit is submitted in support of search and seizure warrants authorizing the search of:

1) A Black Apple iPhone IMEI 359844405482785, SIM 89012606689773049890 7.00 (hereinafter the **SUBJECT TELEPHONE**) as further described in Attachment A-1;
2) A White 2005 Chevrolet Colorado bearing Maryland Registration plates 18W426 (VIN #1GCDT196558153262) (hereinafter the **SUBJECT VEHICLE)** and contents within as further described in Attachment A-2;
3) Records and information associated with certain cellular towers ("cell towers") that are in the possession, custody, and/or control of AT&T, a cellular service provider headquartered at 208 S. Akard Street, Dallas, Texas 75202; T-Mobile, a cellular service provider headquartered at 12920 Se 38th Street, Bellevue, Washington 98006;

Verizon Wireless, a cellular service provider headquartered at One Verizon Way, Basking Ridge, New Jersey 07920; and/or Sprint, a cellular service provider headquartered at 6480 Sprint Parkway, Overland Park, Kansas 66251 (collectively, "**THE SERVICE PROVIDERS**"). as further described in Attachment A-3;

Based upon my training, experience, and knowledge of this investigation, I submit that there is probable cause to believe that violations of 18 U.S.C. § 844(i)&(n) (Arson Affecting Interstate Commerce and Arson Conspiracy) and 18 U.S.C. § 1951 (Use of Threats or Violence to Impede Interstate Commerce) (collectively, "Federal Offenses") have been committed by Dominic Fowler and Dennis Williams, and that evidence and instrumentalities of violations of these explosives and arson laws may be located within the **SUBJECT TELEPHONE, SUBJECT VEHICLE,** and within the information retained by **THE SERVICE PROVIDERS**.

BACKGROUND OF AFFIANT

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and been so since November 2015. Your affiant is an investigative law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 United States Code, and I am empowered by law to conduct investigations and to make arrests for the offenses enumerated in Section 2516 of Title 18 United States Code. Your affiant has received training and experience in interviewing and interrogation techniques, surveillance techniques, arrest procedures, search and seizure, and asset forfeiture. Your affiant also has specific and extensive additional training and experience with explosives and explosive investigations. Your affiant has also been involved in firearms, explosives, gang, wire-taps, organized crime, and drug investigations, including the possession with intent to distribute and distribution of controlled substances, and conspiracies and offenses.

2. Your affiant is presently assigned to Baltimore Group 1 of the Baltimore Field

Division of the ATF. This group is responsible for Arson and Explosives investigations in Maryland and Delaware.

3. In the course of my training and experience, your affiant has become familiar with the methods and techniques associated with the manufacturing, distribution and possession of destructive devices and explosives. In the course of conducting investigations, your affiant has been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses; conducting physical surveillance; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing caller identification system data; and executing search warrants that have led to substantial seizures of narcotics, firearms, and other contraband.

4. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

INTRODUCTION

5. All information contained in this affidavit is either personally known to me or has been related to me by other law enforcement officers and/or other witnesses, or has been obtained from records and documents gathered during the course of this investigation. This affidavit contains information necessary to support probable cause for the search of the **SUBJECT TELEPHONE, SUBJECT VEHICLE,** and within the information retained by **THE SERVICE PROVIDERS**. The information contained in this affidavit is for the limited purpose of supporting the search and is not intended to include each and every fact and matter observed by or known to the affiant.

CELLULAR TELEPHONE DATA

6. Your affiant knows that computers and cellular telephones used by device manufacturers, possessors or users contain valuable information and evidence relating to their manufacturing, possession and/or use. Such information consists of, but is not limited to, call logs,

phone books, photographs, voice mail messages, text messages, images and video, Global Positioning System (GPS) data, browser history, and any other stored electronic data. This information can (i) reflect the preparation for, arrangement of, and commission of the target offenses; (ii) identify locations where device manufacturers, possessors or users traveled to before and after transporting, purchasing or selling destructive devices; (iii) reflect the ownership and use of the computers and cellular telephones by those who use devices; (iv) document meetings and communications between device manufacturers, possessors or users, their customers, associates, and co-conspirators; (v) reflect communications between device manufacturers, possessors or users and other individuals, discussing the manufacturing, use or possession of devices; (vi) reflect communications between device manufacturers, possessors or users and other individuals who may have assisted or provided support in the manufacturer, possession or use of devices; and (vii) document or contain evidence of the obtaining, secreting, manufacturing, transferring, expenditure and/or the concealment of devices relating to the manufacturer, possession or use of devices.

Electronic Storage And Forensic Analysis

7. Based on your affiant's training and experience, your affiant uses the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the

device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A Global Positioning System ("GPS") navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique

numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on your affiant's knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

9. There is probable cause to believe that things that were once stored on the **SUBJECT TELEPHONE** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating

system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

10. *Forensic evidence.* As further described in Attachment B-1, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT TELEPHONE** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT TELEPHONE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore,

contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

11. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your affiant is applying for would permit the examination of the **SUBJECT TELEPHONE** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **SUBJECT TELEPHONE** to human inspection in order to determine whether they contain evidence described by the warrant.

12. *Manner of execution*. Because this warrant seeks only permission to examine devices already in law enforcement possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, your affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

13. This affidavit is based upon information witnessed by your affiant or provided to me by other law enforcement officers/agents, informants, and witnesses, all of whom your affiant believes to be credible. Because this affidavit is being submitted for the limited purpose of securing a search warrant for the aforementioned device, your affiant has not included each and every fact known to him concerning this investigation. Your affiant has set forth only the facts which I believe are necessary to establish probable cause for the issuance of a Search and Seizure Warrant.

HISTORICAL CELL SITE DATA

32. Based on my training and experience, I have learned that **THE SERVICE PROVIDERS** are companies that provide cellular communications service to the general public. In order to provide this service, many cellular service providers maintain antenna towers ("cell towers")

that serve and provide cellular service to devices that are within range of the tower's signals. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data. When sending or receiving communications, a cellular device does not always utilize the cell tower that is closest to it.

33. Based on my training and experience, I also know that each cellular device is identified by one or more unique identifiers. For example, with respect to a cellular phone, the phone will be assigned both a unique telephone number but also one or more other identifiers such as an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The types of identifiers assigned to a given cellular device are dependent on the device and the cellular network on which it operates.

34. Based on my training and experience, I know that cellular service providers, such as **THE SERVICE PROVIDERS,** routinely and in their regular course of business maintain historical records that allow them to determine which wireless devices used cellular towers on the cellular provider's network to send or receive communications. For each communication sent or received via the wireless provider's network, these records may include: (1) the telephone call number and unique identifiers of the wireless device that connected to the provider's cellular tower and sent or received the communication ("the locally served wireless device"); (2) the cellular tower(s) on the provider's network, as well as the "sector" (i.e., face of the tower), to which the locally served wireless device connected when sending or receiving the communication; and (3) the date, time, and duration of the communication. These records may also include the source and destination telephone

numbers associated with the communication (including the number of the telephone that was called or that called the locally served wireless device) and the type of communication (e.g., phone call or SMS text message) that was transmitted.

35. Based on my training and experience, I know that cellular service providers, such as **THE SERVICE PROVIDERS**, have the ability to query their historical records to determine which cellular device(s) connected to a particular cellular tower during a given period of time and to produce the information described above. I also know that cellular providers have the ability to determine which cellular tower(s) provided coverage to a given location at a particular time.

36. Based on my training and experience and the above facts, information obtained from cellular service providers, such as **THE SERVICE PROVIDERS,** that reveals which devices used a particular cell tower (and, where applicable, sector) to engage in particular communications can be used to show that such devices were in the general vicinity of the cell tower at the time the communication occurred. Thus, the records described in Attachment A will identify the cellular devices that were in the vicinity of the **Cell Tower Locations** at the specified time frame of the criminal acts. This information, in turn, will assist law enforcement in determining which person(s) were present or involved with the arson investigation and to identify potential targets and/or witnesses.

14. Based on your affiant's experience, training, and knowledge of this investigation and other investigations to date, individuals committing crimes frequently use cellular telephones, communication devices, and other electronic media storage to further their illegal activities. Through your affiant's training and experience, and participation in this and other arson and other explosives-related investigations, he knows that:

a. The fruits, instrumentalities, and evidence of criminal activity are often concealed in digital form. Electronic devices, such as cellular telephones, frequently contain records including video, pictures, location data and private

messages related to criminal activity. Furthermore, internet searches are often conducted on cellular telephones in reference to how to commit a crime and news stories related to the crime.

b. Individuals planning bombings/explosions often use cellular telephones to maintain telephone number "contact lists" of individuals who may have assisted in the planning of this and other criminal activity.

c. Individuals planning bombings/explosions often use photography and video to document planned location targets, document the criminal activity and identify areas of egress to be used after the commission of the crimes.

d. Finally, based on my training and experience, individuals who commit bombings/explosions, and other criminal activity, often use cellular telephones to communicate with co-conspirators via phone calls and text messages during the preparation, execution, and probable cover up of the explosion.

15. The information to be searched is described in the following paragraphs and in Attachment A-3. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require **THE SERVICE PROVIDERS** to disclose to the government the information further described in Section I of Attachment B-3. Upon receipt of the information described in Section I of Attachment B-3, government-authorized persons will review the information to locate items described in Section II of Attachment B-3.

PROBABLE CAUSE

16. Federal and state law enforcement authorities, including investigators from the ATF, are investigating a series of explosions beginning in August 2022 involving the use of improvised cardboard tube explosive devices similar to pipe bombs (hereinafter "Explosive Device") in connection with thefts from automated teller machines (ATMs) in Maryland. During these incidents, masked suspects will force entry in an establishment and use an Explosive Device to break into and steal money from an ATM. Based on my training, experience, and the evidence gathered to date, it appears that the same group of individuals may be responsible for these crimes.

Incident 1 – Shore United Bank

17. On the morning of August 12, 2022, law enforcement investigators responded to Shore United Bank located at 2151 Defense Highway, Crofton, Maryland 21114 [**Cell Tower Location 1**], following the discovery of an attempted ATM robbery at the location. The investigation revealed that at approximately 12:21 a.m. Eastern Daylight Time (EDT) (NOTE: all times are hereinafter are expressed in EDT unless otherwise noted), two unidentified suspects arrived in the vicinity of the bank in a black Jaguar XJ sedan bearing Virginia registration UFX-5118. At approximately 12:24 a.m. the suspects used pry bars on the ATM and placed an Explosive Device at the base of the ATM in an attempt to break open the machine. The Explosive Device functioned as designed, but was not successful in breaking open the ATM. The suspects departed the area at approximately 12:28 a.m.

Incident 2 – Sunset Mart

18. On the morning of August 12, 2022, law enforcement investigators responded to the Sunset Mart located at 3204 Curtis Drive, Temple Hills, Maryland, 20748 [**Cell Tower Location 2**], following the discovery of an ATM robbery at the location. The investigation revealed that two unidentified suspects arrived in the vicinity of the Sunset Mart in a black Jaguar XJ sedan and forced entry into the establishment. At approximately 1:45 a.m., one suspect is seen cutting the glass of the entry door to the building then departing the area. Approximately one hour later at 2:54 a.m., both suspects returned to the building, made entry, and placed an Explosive Device inside the cash slot of the ATM. The Explosive Device functioned as designed and was successful in breaking open the ATM. However, the ATM only contained $20 dollars in U.S. currency at the time of the robbery, and the suspects departed the area without taking any cash.

19. The suspects were dressed the same at both Incident 1 and Incident 2. Suspect 1 (S1) had a slim and tall build, was wearing glasses, and was dressed in a dark colored hoodie, dark pants,

black and white mechanics gloves, and gray New Balance shoes. Suspect 2 (S2) had a medium build, was dressed in a black hoodie, dark pants, light gray knit gloves dipped in blue rubber latex on the palms and fingers, and black shoes. Both suspects had masks on and their hoods pulled tight around their faces.

Incident 3 – Theft of Chevy Tahoe

20. Home security camera footage captured the theft of a black Chevy Tahoe bearing DC registration GV-2694 from the driveway of a residential property located 1818 Bruce Place SE, Washington DC, 20020 [**Cell Tower Location 3**]. The owner of the vehicle reported it stolen and the police report stated that the event occurred on August 12, 2022, at approximately 5:48 a.m. The video depicts a single individual approach the driveway on foot and check the door handles of two (2) vehicles occupying it, one of which being the black Chevy Tahoe. The suspect is slender, dressed in dark clothing, and wearing light colored tennis shoes which appear to have a reflective "N" on the side consistent with New Balance shoes. The suspect enters the second vehicle in the driveway, then security footage breaks and only shows the Tahoe's brake lights come on and depart the area.

Incident 4 – 7 Summers Liquors

21. On the morning of August 14, 2022, law enforcement investigators responded to 7 Summers Liquors located at 18811 Central Avenue, Bowie, Maryland 20774 [**Cell Tower Location 4**], following the discovery of an ATM robbery at the location. The investigation revealed that two unidentified suspects arrived in the vicinity at approximately 1:41 a.m. in a black Chevy Tahoe bearing DC registration GV-2694 and forced entry into the establishment with pry bars. The suspects placed an Explosive Device inside of the ATM. The Explosive Device functioned as designed and was successful in breaking open the ATM. The suspects took approximately $4,000 dollars in U.S. currency from the machine and departed the area at approximately 1:47 a.m.

22. Security camera footage captured S1 holding an Explosive Device in his hand. The

device appeared to be made of brown cardboard and have a red colored end cap on one end, with a fuse protruding from the other end. The device was shorter and wider, resembling the approximate size of a 12 oz. soda can.

23. The suspects appeared to be dressed in similar clothing to Incidents 1 and 2, including S1 wearing glasses, dark clothing, and gray New Balance shoes, and S2 wearing dark clothing and black shoes. The suspects were wearing light gray knit gloves dipped in blue rubber latex on the palms and fingers. During this incident, security camera footage captured multiple index cards fall out of the rear driver's side door of the Tahoe. Upon arrival at the scene, investigators recovered these cards and placed them into evidence. The cards contained hand-written driving directions to various locations in the area.

Incident 5 – Express Mart

24. On the morning of August 15, 2022, at approximately 6:00 a.m., police officers responded to the Express Mart located at 15709 Hall Road, Bowie, Maryland 20721 [**Cell Tower Location 5**] in reference to a breaking and entering at the location. The officers observed that the store had been ransacked and the ATM had been destroyed. Upon clearing the building and determining it to be safe, the officers informed the store owner that they could clean up. Officers did review security camera footage and learned that two unidentified suspects arrived in the vicinity at approximately 2:07 a.m. in a black Jaguar XJ sedan with Virginia registration UFX-5118 and forced entry into the establishment by cutting the padlocks on the doors and using pry bars. The suspects placed two Explosive Devices inside of the ATM. The Explosive Device functioned as designed and were successful in breaking open the ATM. The suspects took approximately $15,000 dollars in U.S. currency from the machine and departed the area.

25. ATF and state law enforcement investigators responded to the scene on the morning of August 15, 2022, and reviewed the security camera footage. The suspects were dressed similarly

to the previous incidents, including the light gray and blue gloves and dark clothing, except that both had darker colored shoes and one suspect was wearing a bulkier black coat with a hood and small white logo on the left chest. Both suspects had masks on and their hoods pulled tight around their faces. Investigators located one (1) index card in the parking lot of the store with hand-written directions on it, which matched the style of the other cards recovered at the previous incident.

Incident 6 – Arson of Jaguar

26. On August 16, 2022, at approximately 1:56 a.m., Fire Department personnel responded to 4615 Wheeler Hills Road, Oxon Hill, Maryland 20745 [**Cell Tower Location 6**] for the report of a vehicle fire. Fire personnel suppressed the fire and responding police officers called ATF and state law enforcement to investigate. Upon arrival, investigators examined the vehicle and determined it to be a black Jaguar sedan, however, due to fire damage investigators could not determine the model or locate an observable VIN. Upon towing the vehicle, investigators discovered a license plate melted to the engine block which they determined to be Virginia registration UFX-5118, the registration borne by the vehicle used in Incident 1, Incident 2, and Incident 5.

LPR 1 – License Plate Reader Hit

27. On August 25, 2022, at approximately 1:01 a.m., a License Plate Reader (LPR) located at Pennsylvania Ave and 27th St SE in Washington, DC [**Cell Tower Location 7**] captured a black Chevy Tahoe bearing DC registration GV-2694 traveling eastbound toward Maryland.

LPR 2 – Speed Camera Reader Hit

28. On August 25, 2022, at approximately 1:04 a.m., a Speed Camera/License Plate Reader located at 4200 Southern Avenue SE, Capitol Heights, MD 20743 [**Cell Tower Location 8**] captured a black Chevy Tahoe bearing DC registration GV-2694 traveling eastbound toward Maryland.

Incident 7 – Lanham Exxon

29. On the morning of August 25, 2022, law enforcement investigators responded to the Exxon station located at 9500 Lanham Severn Road, Lanham, Maryland 20706 [**Cell Tower Location 9**], following the discovery of an ATM robbery at the location. The investigation revealed that two unidentified suspects arrived in the vicinity at approximately 1:56 a.m. in a black Chevy Tahoe bearing DC registration GV-2694 and forced entry into the establishment using pry bars. The suspects placed an Explosive Device inside of the ATM. The Explosive Device functioned as designed and was successful in breaking open the ATM. The suspects took an unknown quantity of currency from the machine and departed the area at approximately 1:58 a.m.

30. S1 appeared to have a medium build, was wearing a dark colored hoodie, black and gray gloves, dark colored pants, black leather shoes, and had a key ring attached to his front belt loop. S2 appeared to have a medium build and was wearing a bulkier black coat with a hood and a small white logo on the left chest, dark colored pants, light gray knit gloves dipped in blue rubber latex on the palms and fingers, and black shoes with a possible light-colored logo near the heel. The suspects used pry bars to gain entry in the building and into the ATM. S1 placed an Explosive Device in the machine and S2 appeared to have a second Explosive Device in his hand which was not used. The device which S1 placed in the machine appeared to be long and narrow with an orange-red colored cardboard exterior, while the device which S2 held in his hand appeared to be made of brown cardboard and was shorter and wider, resembling a 12 oz. soda can.

Incident 8 – Glenn Dale Mini-Mart

20. On the afternoon of August 25, 2022, law enforcement investigators recovered security footage from the Glen Dale Mini-Mart/Crown station located at located at 11002 Lanham Severn Road, Glenn Dale, Maryland 20769 [**Cell Tower Location 10**]. The footage showed two unidentified suspects arrived in the vicinity at approximately 2:08 a.m. in a black Chevy Tahoe and

attempt to force entry into the establishment. S1 first attempted to use a possible window punch to break the front glass but was not successful. The suspects then attempted to use bolt cutters to break the glass on the store but were not successful. The suspects were dressed in the same clothing as the previous incident, which had occurred approximately 10 minutes prior. The suspects departed the area in the Tahoe and did not breach the structure.

Incident 9 – Fat Boys Crab Shack

21. On the morning of August 25, 2022, law enforcement investigators responded to Fat Boys Crab Shack located at 1581 Defense Highway, Gambrills, Maryland 21054 [**Cell Tower Location 11**] following the discovery of an ATM robbery at the location. Investigators were not able to recovery security camera footage from the establishment, however, the security system burglar alarm was triggered at 2:46 a.m. followed by the building's fire alarm system. The Explosive Device functioned as designed and was successful in breaking open the ATM. The suspects took approximately $3,100 dollars in U.S. currency from the machine.

22. Investigators collected evidence from the scene which included pry bar tool marks on the entry door jam, plastic pieces believed to be part of the end cap to the Explosive Device, and pieces of brown cardboard believed to be from the Explosive Device itself. At the previously associated incidents, pry bars have been used on the entry doors and investigators have recovered plastic pieces and pieces of brown cardboard consistent with the evidence collected from this incident.

LPR 2 – License Plate Reader Hit

23. On August 25, 2022, at approximately 3:02 a.m., a License Plate Reader (LPR) located at MD-295 s/b and Eastern Avenue NE in Washington DC [**Cell Tower Location 12**] captured a black Chevy Tahoe bearing DC registration GV-2694 traveling southbound into Washington DC.

Recovery of Tahoe

24. On September 6, 2022, at approximately 1:30 a.m., Washington DC Metro Police Officers located and recovered the black Chevy Tahoe bearing DC registration GV-2694 parked unoccupied in Southeast DC. Law enforcement officers associated with this investigation followed the vehicle and took possession of it pending a search and seizure warrant.

Incident 10 – Theft of Chevy Colorado

25. On September 12, 2022, at approximately 3:50 a.m., a white 2005 Chevy Colorado (**SUBJECT VEHICLE**) bearing Maryland registration 18W426 was stolen from the residential property located at 3582 Riva Road, Davidsonville, MD 21035 [**Cell Tower Location 13**]. Security camera footage from the property captured the headlights of an unknown vehicle in the driveway at approximately 2:59 a.m. and additional unknown activity around the Chevy Colorado was seen at 3:19 a.m. At approximately 3:50 a.m. the headlights to the Chevy Colorado turned on, and the vehicle left the property.

Incident 11 – Footage of Stolen Colorado

26. On September 12, 2022, at approximately 3:53 a.m., security camera footage from a CITGO gas station located 801 W Central Avenue, Davidsonville, MD 21035 [**Cell Tower Location 14**] captured the **SUBJECT VEHICLE** traveling westbound with an unknown dark colored follow-car behind it.

27. On September 12, 2022, at approximately 3:53 a.m., security camera footage from a Davidsonville Elementary School located 962 W Central Avenue, Davidsonville, MD 21035 [**Cell Tower Location 15**] captured the **SUBJECT VEHICLE** traveling westbound with an unknown dark colored follow-car behind it.

Incident 12 – Jumbo Foods International

28. On the morning of September 13, 2022, law enforcement responded to Jumbo Foods

International located at 3201 Brinkley Road Temple Hills, Prince George's County, Maryland 20748 [**Cell Tower Location 16**], following the report of an ATM robbery at the location. The investigation revealed that two unidentified suspects arrived in the vicinity at approximately 3:44 a.m. in the **SUBJECT VEHICLE** and forced entry into the secured building. The suspects placed an Explosive Device inside of the ATM to break open the machine. The Explosive Device failed to function and the suspects fled from the property, leaving the device behind.

29. The suspects were dressed similarly to previous incidents. S1 appeared to be slim and was wearing dark clothing and gray New Balance shoes, S2 was wearing dark clothing and black shoes.

30. Approximately three (3) hours later at 6:55 a.m. on the same date, the suspects returned in the **SUBJECT VEHICLE** and re-entered the structure. The suspects placed an additional Explosive Device inside of the ATM. The Explosive Device functioned as designed and opened the ATM. The suspects reportedly took approximately $5,500 dollars U.S. currency from the machine then departed the area.

31. When the suspects returned, they were dressed in similar dark clothing, however, both suspects were in black shoes.

32. When law enforcement arrived at the incident they recovered the intact Explosive Device which the suspects had left at the scene earlier that morning. The device was made of brown cardboard and had a red colored end cap on one end with a fuse protruding from the other end. The device was shorter and wider, resembling a 12 oz. soda can.

Incident 13 – Urban Market/All Saints Liquors

33. On the morning of September 13, 2022, law enforcement responded to the Urban Market located at 9105-B All Saints Road, Laurel, Howard County, Maryland 20707 [**Cell Tower Location 17**] following the discovery of an ATM robbery at the location. The investigation revealed

that two unidentified suspects arrived in the vicinity at approximately 4:33 a.m. in the **SUBJECT VEHICLE**. The suspects exited the truck and looked into the front window of 9105-N, All Saints Liquors. The suspects then proceeded to 9105-B, Urban Market, and forced entry into the secured building. The suspects initially threw bricks/concrete blocks at the glass door then used a pry bar to gain entry. Once inside the suspects placed an Explosive Device inside of the ATM. The Explosive Device functioned as designed and the suspects were successful in obtaining U.S. currency from the machine. The suspects appeared to be dressed in the same clothing as the previous incident approximately one hour earlier.

Mobilization of the Chevy Colorado

34. Having previously installed a GPS tracker on **SUBJECT VEHICLE**, which had been stolen in Anne Arundel County (see paragraph 27 above), after it was located parked near 3956 Martin Luther King Jr Ave SW, Washington DC, 20032 [**Cell Tower Location 18]** investigators became aware that the **SUBJECT VEHICLE** had begun moving at approximately 12:56 a.m. on the morning of September 29, 2022. Law enforcement officers mobilized to follow the GPS pings from the tracker and were able to locate the **SUBJECT VEHICLE.**

Incident 14 – Global Food

35. On the morning of September 29, 2022, law enforcement responded to Global Food located at 5470 Saint Barnabas Road, Prince George's County, Maryland 20745 [**Cell Tower Location 19**] for an ATM robbery at the location. As a result of following the GPS ping alert described in paragraph 34, law enforcement officers were in the area during the incident and were able to apprehend two (2) individuals associated with the robbery, identified as Dominic FOWLER and Dennis WILLIAMS.

36. Law enforcement officers were tracking the **SUBJECT VEHICLE** as it arrived in the vicinity of Global Food at approximately 2:55 a.m. The driver, FOWLER, exited the vehicle and

breached the front door of Global Food, while the passenger, identified as WILLIAMS, remained in the truck to act as a look-out. FOWLER initially attempted to use a brick to break the glass of the door but was unsuccessful, he then returned to the truck, retrieved a pry bar, and was successfully in prying the door open. FOWLER then proceeded directly to the ATM, used a pry bar on the machine and placed an Explosive Device inside of it. FOWLER lit the Explosive Device and it functioned as designed. As FOWLER lit the device, WILLIAMS noticed law enforcement officers approaching and honked the vehicle's horn to warn FOWLER. FOWLER re-entered the driver's seat of the **SUBJECT VEHICLE** and attempted to flee the area but was apprehended by law enforcement.

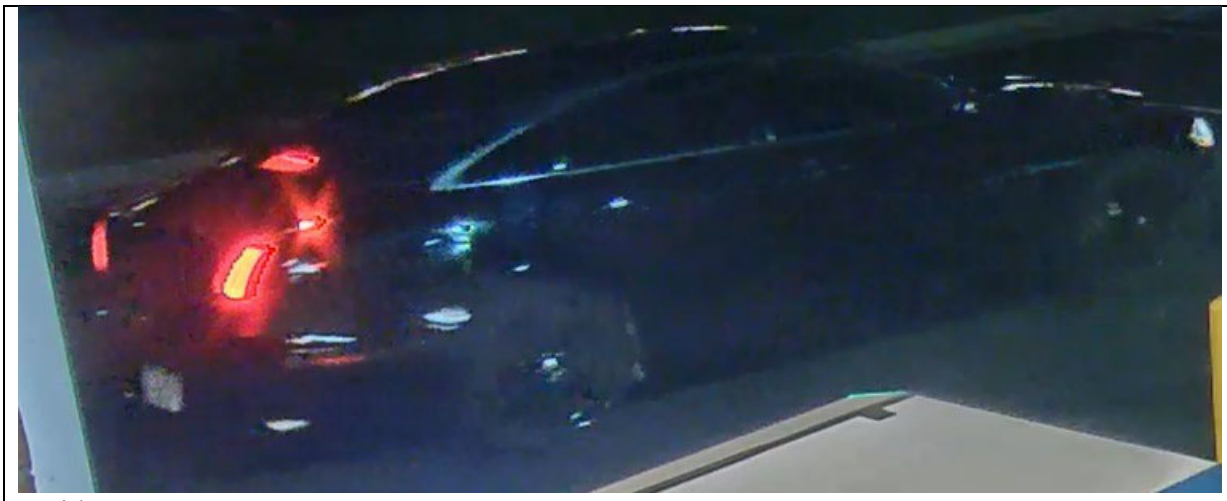
31. While WILLIAMS waited in the **SUBJECT VEHICLE**, he appeared to hold something in his hand which glowed and was consistent in size and shape to a cellular phone. FOWLER, who has a tall and slender build, was dressed in similar clothing to previous incidents including a dark colored hooded sweatshirt pulled tight over his face, a mask, dark colored pants, gloves, and gray New Balance shoes.

32. Due to the dangerous nature of explosives, law enforcement Bomb Technicians conducted a safety sweep of the **SUBJECT VEHICLE** and recovered an additional, intact Explosive Device from within the **SUBJECT VEHICLE**. The recovered device was made of brown cardboard, had a red colored end cap on one end, and a fuse protruding from the other end. The device was shorter and wider, resembling a 12 oz. soda can.

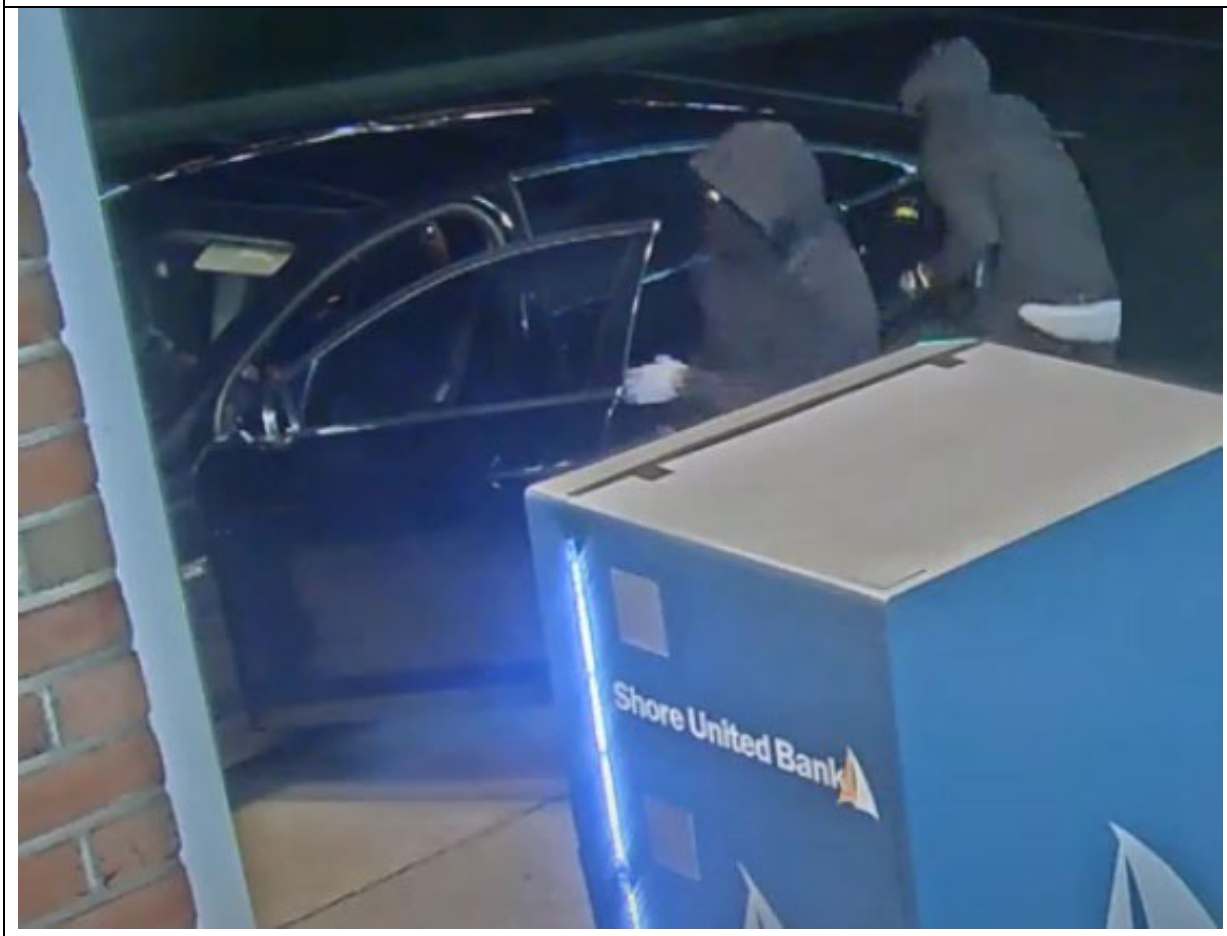
Surveillance Video

33. Investigators have recovered surveillance video related to the robberies from most of the locations. Review of the surveillance video from Incident 2 (Shore United Bank) and Incident 3 (Sunset Mart) revealed both suspects wearing the same clothing at each location, including dark colored hooded top, dark pants, and masks with their hoods pulled tight. S1 was a slim build and wearing gray New Balance shoes, black and white mechanics gloves, and glasses. S2 was a medium

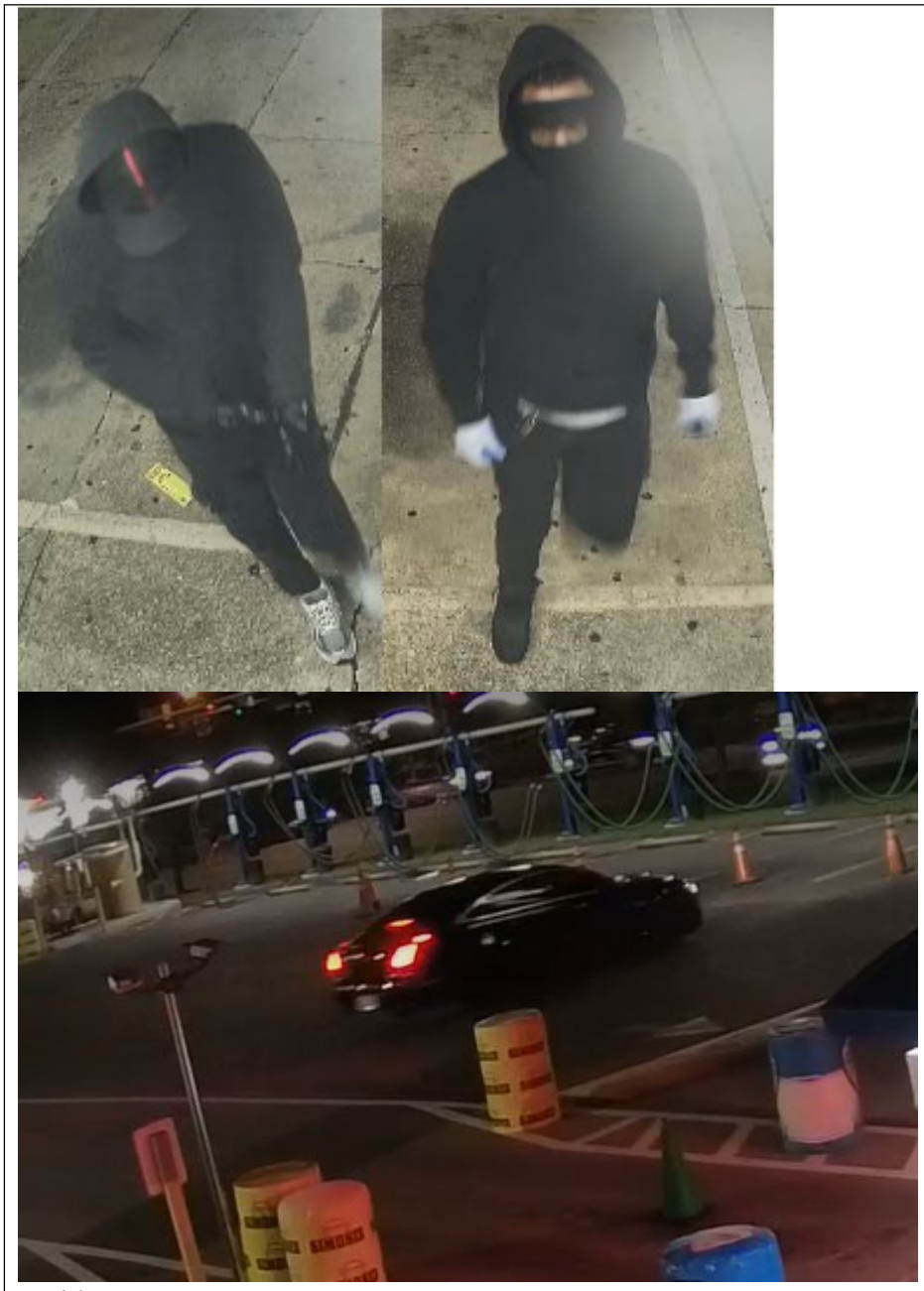
build and wearing a black hoodie, light gray knit gloves dipped in blue rubber latex on the palms and fingers, and black leather shoes



Incident 1



Incident 2



Incident 3

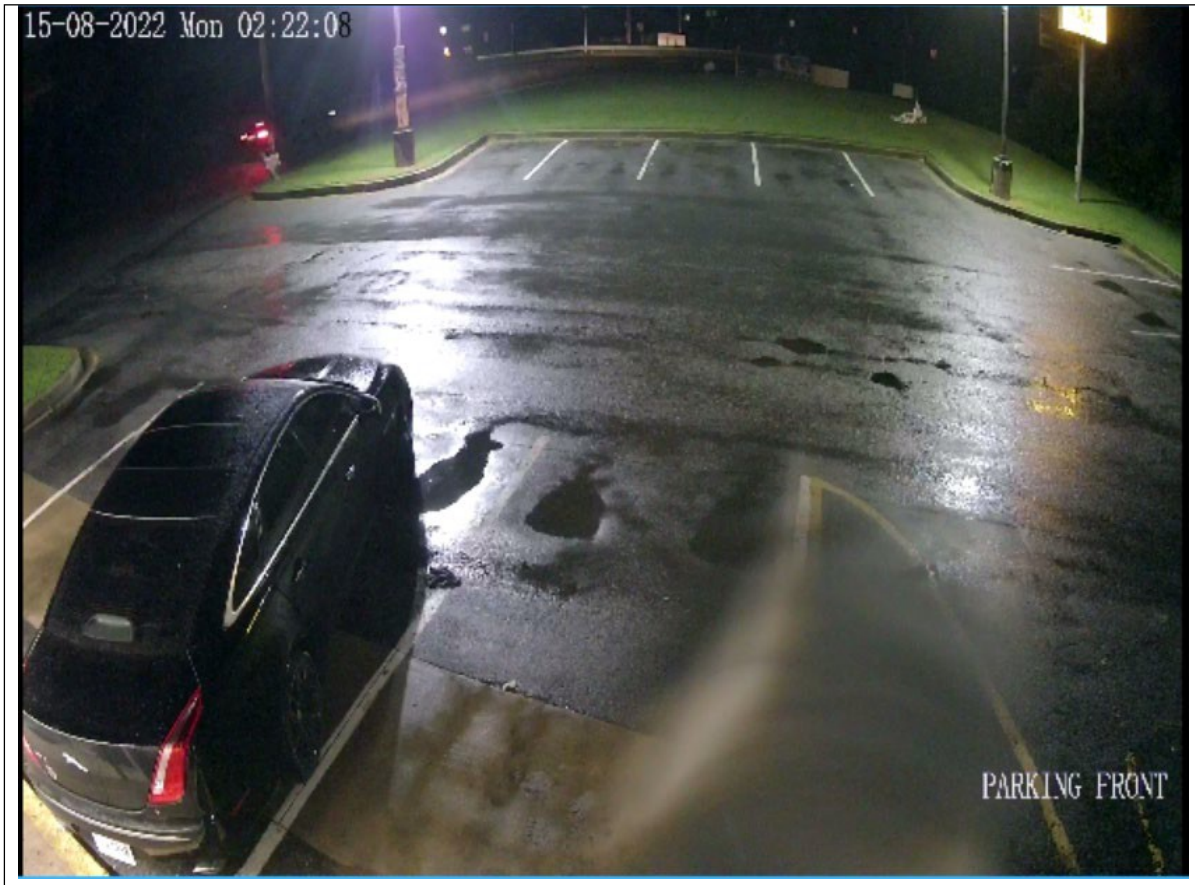
34. Review of the surveillance video from the Incident 4 (7 Summers Liquors) revealed S1 wearing a dark gray hoodie, light gray knit gloves dipped in blue rubber latex on the palms and fingers, glasses, and light gray New Balance shoes, and S2 wearing a black hoodie, light gray knit gloves dipped in blue rubber latex on the palms and fingers, and black leather shoes. This clothing appeared to be very similar to the clothing used at Incident 2 and Incident 3. At this location the

suspects used a Chevy Tahoe and several index cards with directions written on them fell from the door of the vehicle.

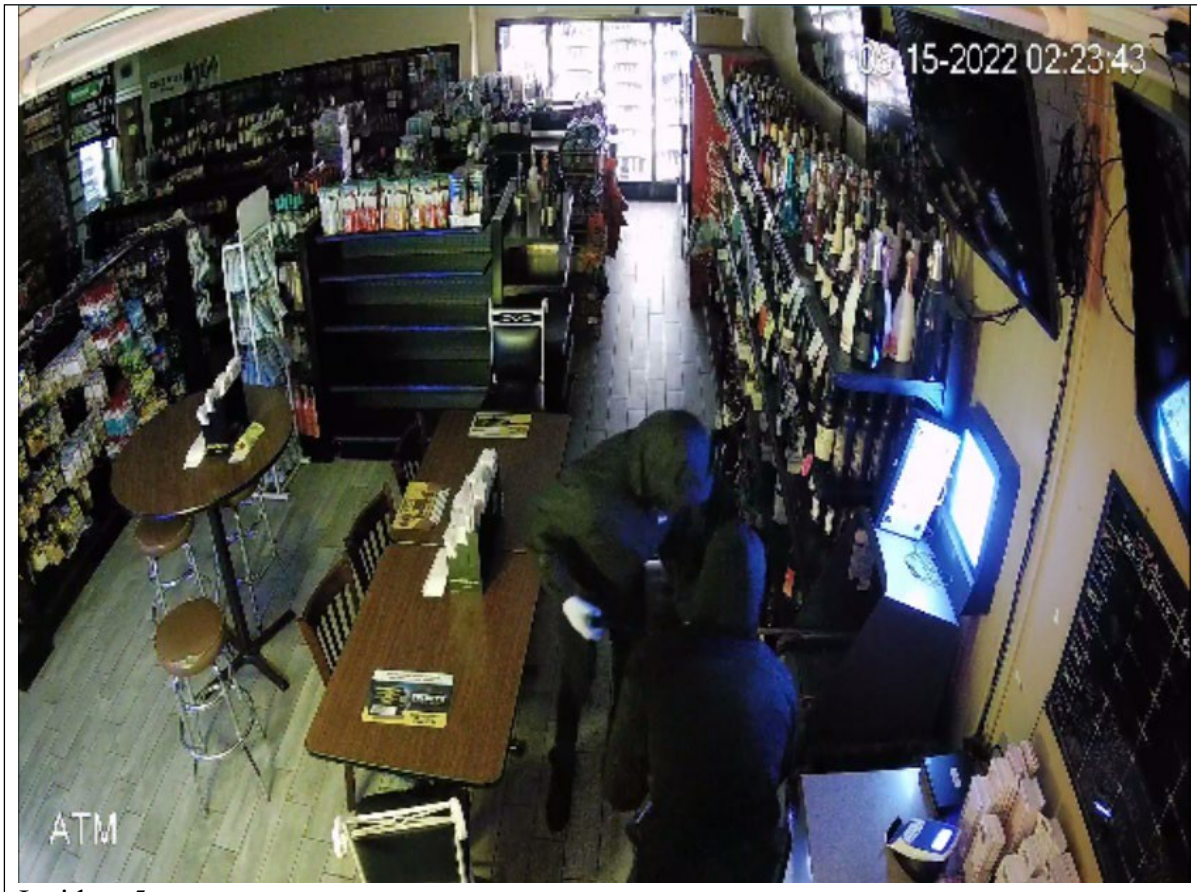
Incident 4

Incident 4 (Explosive Device visible in hand)

35. Review of the surveillance video from Incident 5 (Express Mart) revealed S1 wearing a dark colored hoodie, dark pants, and dark shoes. S2 was wearing a bulkier dark coat, dark pants, and dark shoes. This clothing appeared to be very similar to the clothing used at Incident 4 and the gloves appeared to be the same light gray knit gloves dipped in blue rubber latex on the palms and fingers. Of note, however, is that S2 was wearing a bulkier black hooded coat with a small white logo on the left chest while. At this location the suspects used the black Jaguar and investigators discovered one index card with directions written on it in the parking lot.

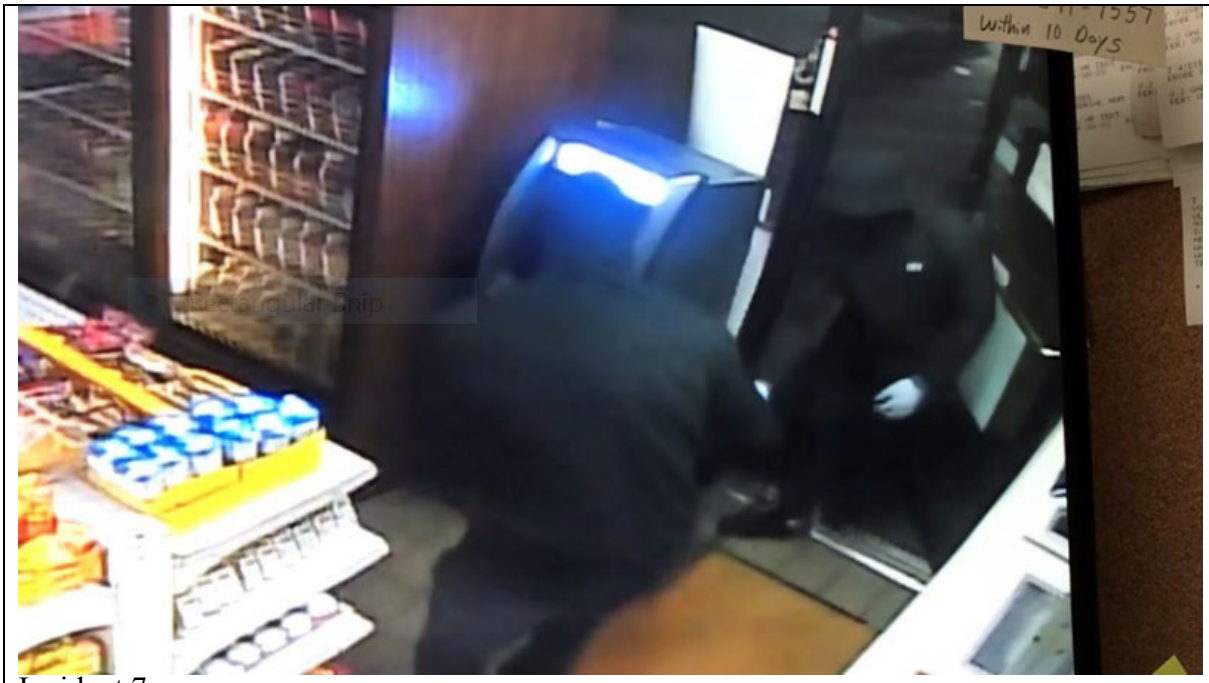


Incident 5

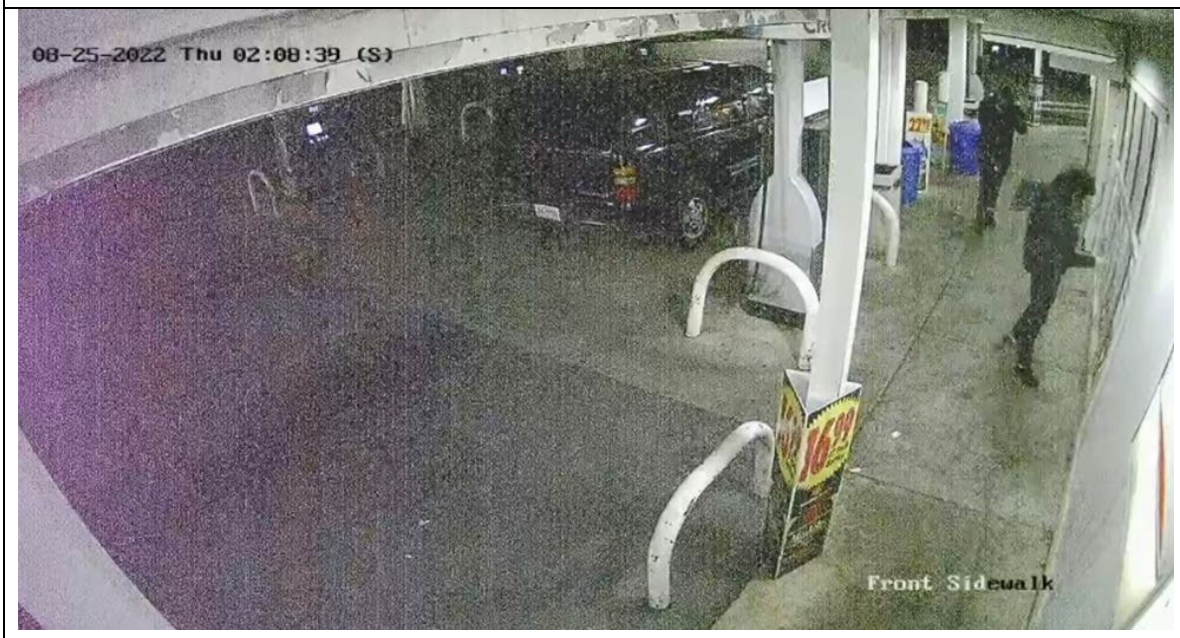


Incident 5

36. Review of the surveillance video from Incident 7 (Exxon Station) and Incident 8 (Glen Dale Mini-Mart) revealed the suspects wearing very similar clothing to the clothing during at Incident 5. Of note are the light gray knit gloves dipped in blue rubber latex on the palms and fingers and S2 wearing the bulkier black hooded coat with small white logo on the left chest. At these locations the suspects used the Chevy Tahoe.



Incident 7



Incident 8

37. Review of the surveillance video from Incident 12 (Jumbo Foods) and Incident 13 (Urban Market) revealed S1 wearing a dark colored hoodie, dark pants, dark gloves, and tennis shoes gray New Balance shoes, and S2 was wearing dark clothing, a bulkier black coat with a small white logo on the left chest, and tennis shoes. During Incident 13, S2 assisted with breaching the door,

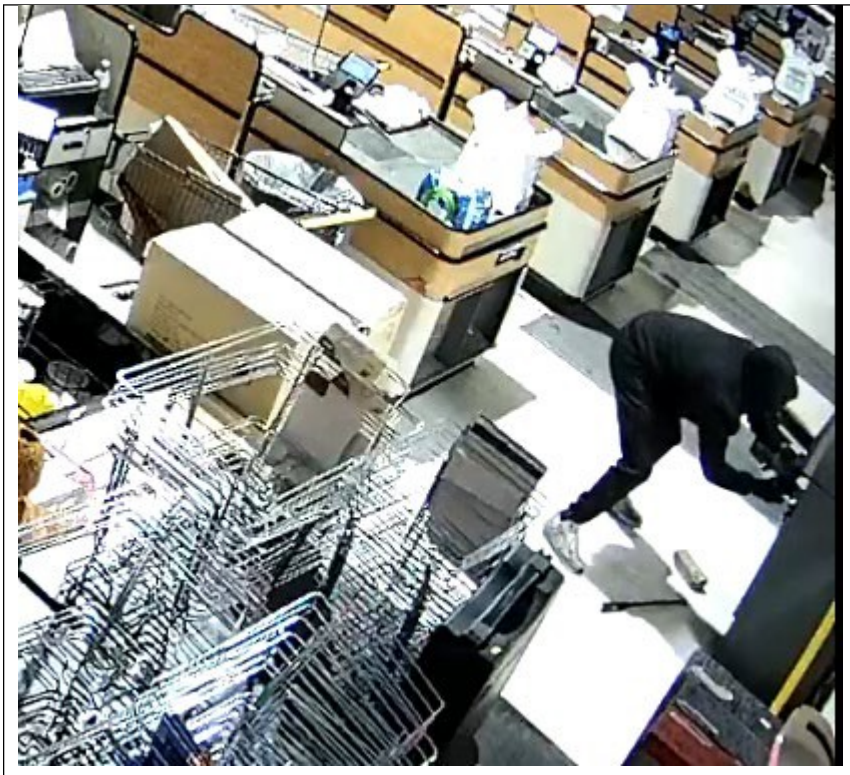
however, remained outside of the building while S1 pried open the ATM and initiated the Explosive Device.

38. When the suspects returned to Incident 12 (Jumbo Foods) at approximately 6:55 a.m. the suspect who ran inside to initiate the new Explosive Device was dressed similarly but was wearing black shoes. At these locations the suspects used the **SUBJECT VEHICLE**.

Incident 13

Incident 13 (Explosive Device visible on floor)

39. At Incident 14 (Global Food), S1 (identified as FOWLER) was wearing dark colored clothing and gray New Balance shoes similar to the previously associated incidents. Unlike the previous incidents, FOWLER executed the robbery of the ATM alone while WILLIAMS remained in the vehicle.



FOWLER at Incident 14

Incident 14

40. When FOWLER was placed into custody, he had items on his person including a window punch, a flashlight, several hundred dollars in U.S. currency, and the **SUBJECT TELEPHONE.** The **SUBJECT VEHICLE** was towed to a secured police location pending a search warrant.

AUTHORIZATION REQUEST

41. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41, based on a finding that there is probable cause to believe that these arson and burglary events are related and committed by overlapping, if not identical, groups of subjects who can be more fully identified through the information sought by this search warrant.

42. I request that the Court direct **THE SERVICE PROVIDERS** to disclose to the government any information described in Section I of Attachment B-3 that is within its possession, custody, or control. Because the warrant will be served on **THE SERVICE PROVIDERS**, who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

43. Furthermore, I submit that the **SUBJECT TELEPHONE** may contain the records of the most recent calls, which may include calls with persons involved in the offense(s). The **SUBJECT TELEPHONE** may contain copies of SMS or text or other electronic communications relating to activities associated with the offense(s). The **SUBJECT TELEPHONE** may also contain a variety of other electronic evidence, including electronic communications through various cellular or internet-based applications, photographs and other information.

44. Finally, I respectfully submit that there is probable cause to believe that FOWLER and WILLIAMS used the **SUBJECT VEHICLE** to unlawfully store and transport explosives, in

violation of the associated offenses. I further submit that the **SUBJECT VEHICLE** may contain contents within which further identify the occupants, including but not limited to paperwork, identification cards, electronic devices, and cellular phones. Your affiant believes there is probable cause and respectfully requests the Court grant investigators permission to search any electronic devices and cellular phones recovered from within the **SUBJECT VEHICLE** for contents as described in Attachment B-1.

CONCLUSION

45. Your affiant alleges the aforementioned facts show that there is probable cause to believe that fruits, evidence, and instrumentalities of violations of the explosives and arson laws, specifically, 18 U.S.C. § 844(i)&(n) (Arson Affecting Interstate Commerce and Arson Conspiracy) and 18 U.S.C. § 1951 (Use of Threats or Violence to Impede Interstate Commerce) committed by Dominic FOWLER and Dennis WILLIAMS, are confined to the **SUBJECT TELEPHONE**, the **SUBJECT VEHICLE,** and the information retained by **THE SERVICE PROVIDERS**.

46. Wherefore, in consideration of the facts presented, I respectfully request that this Court issue a search warrant for the **SUBJECT TELEPHONE**, and authorize the search of the item described in Attachment A-1, for the information set forth in Attachment B-1, a search warrant for the **SUBJECT VEHICLE**, and authorize the search of the item described in Attachment A-2, for the information set forth in Attachment B-2, and a search warrant for **THE SERVICE PROVIDERS**, and authorize the search of the item described in Attachment A-3, for the information set forth in Attachment B-3.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Respectfully submitted,

BENJAMIN PARKER Digitally signed by BENJAMIN PARKER
Date: 2022.10.05 13:06:37 -04'00'

Benjamin D. Parker
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

Affidavit submitted by email and attested as true and accurate by telephone, consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) on this 6th day of October, 2022.

Honorable Ajmel A. Quereshi
United States Magistrate Judge

ATTACHMENT A-1

Property to be searched

The device currently **in** the custody of the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") located at the ATF Baltimore Field Office at 31 Hopkins Place, Baltimore:

- Black Apple iPhone IMEI 359844405482785, SIM 8901260668977304989 07.00

ATTACHMENT A-2

Property to be Searched

The vehicle currently **in** the custody of the Prince George's Police Department located at 8801 Police Plaza, Upper Marlboro, Maryland

The property to be searched is a white **2005 Chevrolet Colorado** bearing Maryland Registration plates 18W426, VIN #1GCDT196558153262, stolen from Anne Arundel County, Maryland, and used by Dominic FOWLER and Dennis WILLIAMS.

ATTACHMENT A-3

Property to be Searched

This warrant applies to records and information associated with communications to and from the following the cellular towers ("cell towers") on the identified dates and timeframes that are within the possession, custody, or control of the cellular service providers identified below:

Cell Towers	Dates	Times
Cell Tower Location 1: The cellular towers that provided cellular service to **2151 Defense Highway, Crofton, Maryland 21114**	August 12, 2022	12:01 a.m. – 1:00 a.m. EDT
Cell Tower Location 2: The cellular towers that provided cellular service to **3204 Curtis Drive, Temple Hills, Maryland, 20748**	August 12, 2022	1:30 a.m. – 3:30 a.m. EDT
Cell Tower Location 3: The cellular towers that provided cellular service to **1818 Bruce Place SE, Washington DC, 20020**	August 12, 2022	5:00 a.m. – 6:15 a.m. EDT
Cell Tower Location 4: The cellular towers that provided cellular service to **18811 Central Avenue, Bowie, Maryland 20774**	August 14, 2022	1:00 a.m. – 2:00 a.m. EDT
Cell Tower Location 5: The cellular towers that provided cellular service to **15709 Hall**	August 15, 2022	1:45 a.m. – 2:45 a.m. EDT

Road, Bowie, Maryland 20721		
Cell Tower Location 6: The cellular towers that provided cellular service to **4615 Wheeler Hills Road, Oxon Hill, Maryland 20745**	August 16, 2022	12:30 a.m. – 2:00 a.m. EDT
Cell Tower Location 7: The cellular towers that provided cellular service to **Pennsylvania Ave and 27th St SE in Washington DC (38.872749, -76.968987)**	August 25, 2022	12:56 a.m. – 1:06 a.m. EDT
Cell Tower Location 8: The cellular towers that provided cellular service to **4200 Southern Avenue SE, Capitol Heights, MD 20743 (38.8672560, -76.9424511)**	August 25, 2022	12:58 a.m. – 1: 08 a.m. EDT
Cell Tower Location 9: The cellular towers that provided cellular service to **9500 Lanham Seabrook Road, Lanham, Maryland 20706**	August 25, 2022	1:45 a.m. – 2:05 a.m. EDT
Cell Tower Location 10: The cellular towers that provided cellular service to **11002 Lanham Severn Road, Glenn Dale, Maryland 20769**	August 25, 2022	2:00 a.m. – 2:20 a.m. EDT
Cell Tower Location 11: The cellular towers that provided cellular service to **1581 Defense**	August 25, 2022	2:30 a.m. – 3:00 a.m. EDT

Highway, Gambrills, Maryland 21054		
Cell Tower Location 12: The cellular towers that provided cellular service to **MD-295 s/b and Eastern Avenue NE in Washington DC (38.909822, -76.935704)**	August 25, 2022	2:57 a.m. – 3:07 a.m. EDT
Cell Tower Location 13: The cellular towers that provided cellular service to **3582 Riva Road, Davidsonville, MD 21035**	September 12, 2022	2:00 a.m. – 4:00 a.m. EDT
Cell Tower Location 14: The cellular towers that provided cellular service to **801 W Central Avenue, Davidsonville, MD 21035**	September 12, 2022	3:45 a.m. – 4:00 a.m. EDT
Cell Tower Location 15: The cellular towers that provided cellular service to **962 W Central Avenue, Davidsonville, MD 21035**	September 12, 2022	3:45 a.m. – 4:00 a.m. EDT
Cell Tower Location 16: The cellular towers that provided cellular service to **3201 Brinkley Road Temple Hills, Prince George's County, Maryland 20748**	September 13, 2022	2:45 a.m. – 4:15 a.m. EDT, and 6:00 a.m. – 7:15 a.m. EDT
Cell Tower Location 17: The cellular towers that provided cellular service to **9105-B All**	September 13, 2022	3:30 a.m. – 5:00 a.m. EDT

Saints Road, Laurel, Howard County, Maryland 20707		
Cell Tower Location 18: The cellular towers that provided cellular service to **3956 Martin Luther King Jr Ave SW, Washington DC, 20032**	September 28, 2022	12:01 a.m. – 1:15 a.m. EDT
Cell Tower Location 19: The cellular towers that provided cellular service to **5470 Saint Barnabas Road, Prince George's County, Maryland 20745**	September 28, 2022	2:30 a.m. – 3:00 a.m. EDT

THE SERVICE PROVIDERS, as listed below, are required to disclose information to the United States pursuant to this warrant.

1. AT&T, a cellular service provider headquartered at 208 S. Akard Street, Dallas, Texas 75202;
2. T-Mobile, a cellular service provider headquartered at 12920 Se 38th Street, Bellevue, Washington 98006;
3. Verizon Wireless, a cellular service provider headquartered at One Verizon Way, Basking Ridge, New Jersey 07920; and
4. Sprint, a cellular service provider headquartered at 6480 Sprint Parkway, Overland Park, Kansas 66251.

ATTACHMENT B-1

Property to be seized

All information and data contained within the device, since August 2022, to include, but not limited to fruits, evidence, information relating to, contraband, or instrumentalities, in whatever form and however stored, relating to evidence and instrumentalities of violations of federal laws, specifically, of 18 U.S.C. § 844(i)&(n) (Arson Affecting Interstate Commerce and Arson Conspiracy) and 18 U.S.C. § 1951 (Use of Threats or Violence to Impede Interstate Commerce) (the "target offenses"). Specifically, as described in the search warrant affidavit, including, but not limited to, call logs, phone books, photographs, voice mail messages, text messages, images and video, Global Positioning System data, and any other stored electronic data:

(i) establishing or documenting the preparation to commit or the commission of the target offenses;

(ii) identifying locations where the individual committed the target offenses, traveled to before and after the commission of the target offenses, and in preparation for the target offenses;

(iii) reflecting the ownership and use of the items identified in Attachment A by the individual committing the target offenses;

(iv) documenting meetings and communications between individuals committing one or more of the target offenses;

(v) reflecting communications between the individual committing one or more of the target offenses and other individuals, discussing the commission of one or more of the target offenses;

(vi) reflecting communications between the individual committing one or more of the target offenses and other individuals who may have assisted or provided support in the commission of one or more of the target offenses;

(vii) containing photographs or video that would constitute evidence of a violation of the target offenses;

(viii) documenting or containing evidence of the manufacturing, obtaining, secreting, transfer, expenditure and/or the concealment of explosives, which would constitute evidence of one of the target offenses; and

(ix) documenting or containing evidence of the purchase of items from the assets derived from the commission of an arson or explosives trafficking offense in violation of 18 U.S.C. § 844(i)&(n) (Arson Affecting Interstate Commerce and Arson Conspiracy) and 18 U.S.C. § 1951 (Use of Threats or Violence to Impede Interstate Commerce) which would constitute evidence of one of the target offenses.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect if from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B-2

Property to be Seized

The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of Title 18 U.S.C. §§ of 18 U.S.C. § 844(i)&(n) (Arson Affecting Interstate Commerce and Arson Conspiracy) and 18 U.S.C. § 1951 (Use of Threats or Violence to Impede Interstate Commerce) (the "TARGET OFFENSES").

1. Evidence establishing or documenting the preparation to commit or the commission of the target offenses;

2. Documents or electronic evidence identifying locations where the individual committed the target offenses, traveled to before and after the commission of the target offenses, and in preparation for the TARGET OFFENSES;

3. Communications between the individual committing one or more of the TARGET OFFENSES and other individuals, discussing the commission of one or more of the TARGET OFFENSES;

4. Evidence of the manufacturing, obtaining, secreting, transfer, expenditure and/or the concealment of explosives, which would constitute evidence of one of the TARGET OFFENSES; and

5. Evidence of the purchase of items from the assets derived from the commission of an arson or explosives trafficking offense in violation of 18 U.S.C. § 844(i)&(n) (Arson Affecting Interstate Commerce and Arson Conspiracy) and 18 U.S.C. § 1951 (Use of Threats or Violence to Impede Interstate Commerce) which would constitute evidence of one of the target offenses.

6. Weapons, including but not limited to revolvers, semi-automatic pistols, rifles and ammunition, ammunition, magazines, bulletproof vests, and firearms-related paraphernalia including, but not limited to, gun-cleaning kits, gun-sights, holsters, receipts and documentation for the purchased of same, and related firearm paraphernalia, which constitute tools for the commission of the TARGET OFFENSES.

7. Clothing worn by D. FOWLER, and D. WILLIAMS and their associates during or in relation to the TARGET OFFENSES, as well as any items containing potential DNA or fingerprint evidence related to FOWLER or WILLIAMS.

8. Address and/or telephone books and papers reflecting names, addresses and/or telephone numbers, which constitute evidence of customers, distributors, conspirators, and potential witnesses of violations of the TARGET OFFENSES.

9. Books, records, receipts, bank statements, money drafts, letters of credit, money orders and cashier's checks, passbooks, bank checks, safe deposit box keys, and any other items

evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money, which constitute records and proceeds of the TARGET OFFENSES.

10. United States currency which constitutes proceeds of the TARGET OFFENSES.

11. Photographs, in whatever form, of co-conspirators, explosive devices, combustible materials, firearms, tools, and proceeds, which constitute evidence of the TARGET OFFENSES.

12. Evidence of relationships between D. FOWLER, and D. WILLIAMS, including evidence of identification and evidence of motivation to engage in arson and burglary or the unlawful possession of explosive devices.

13. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the specified TARGET OFFENSES. The following definitions apply to the terms as set out in this Affidavit and attachment:

a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. Documentation: Computer related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test"

keys or "hot" keys, which perform certain pre set security functions when touches. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

14. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

15. With respect to the search of any of the items described above which are stored in the form

of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

f. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

16. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B-3

Particular Things to be Seized

I. Records and Other Information to Be Disclosed by the Provider

For each cell tower described in Attachment A, **THE SERVICE PROVIDERS** identified in Attachment A are required to disclose to the United States all records and other information (not including the contents of communications) about all communications made using the cell tower(s) identified in Attachment A during the corresponding timeframe(s) listed in Attachment A, including the records that identify:

a. the telephone call number and unique identifiers for each wireless device in the vicinity of the tower ("the locally served wireless device") that registered with the tower, including Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), and International Mobile Equipment Identities ("IMEI");

b. the source and destination telephone numbers associated with each communication (including the number of the locally served wireless device and the number of the telephone that called, or was called by, the locally served wireless device);

c. the date, time, and duration of each communication;

d. the "sectors" (i.e., the face(s) of the tower(s)) that received a radio signal from each locally served wireless device; and

e. the type of communication transmitted through the tower (such as phone call, text message, or data).

These records should include records about communications that were initiated before or terminated after the specified time periods, as long as part of the communication occurred during the relevant time periods identified in Attachment A.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 844(i) (arson affecting interstate commerce), 18 U.S.C. § 844(n) (conspiracy to commit arson) and 18 U.S.C. § 1951 (interference with commerce by threats or violence) during the period of August, 2022, through present.

With respect to the search of the information provided pursuant to this warrant by the above referenced providers, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by **THE SERVICE PROVIDERS** in order to locate the things particularly described in this Warrant.